Remarks

Claims 1-37 have been canceled, and new claims 38-49 presented.

Method claims 1-3, 7-10, 12, 15 and 19-20 were rejected under 35 USC 101 and have been canceled above.

Claims 1, 7-10, 15, 19-20 and 25-37 were rejected under 35 USC 102(e) based on US 7,552,480 to Voss. Applicants respectfully traverse this rejection as applied to new claims 38-49, based on the following.

Voss assesses a security risk based on (a) threat of attack based on possible "threat agents", (b) possible mode of access to a computer system, and (c) privilege components of one or more vulnerabilities to a computer system. The possible "threat agents" are casual users, kiddy scriptors, hackers, disgruntled employees, legitimate consumers, competitors, political activists, agents of organized crime, law enforcement agents, or government agents. The possible modes of access include wide area network access, global network access, wireless access, proprietary network access, packet switched network access, terminal access, and physical access. More specifically, Voss teaches:

> "A numerical value is established for one or more threats of attack on an information system asset of the entity based on expert knowledge without reference to actuarial data. Likewise, based on expert knowledge without reference to actuarial data, **a numerical value is established for each of one or more access and privilege components of one or more vulnerabilities to attack on the information system asset.** Based upon the numerical values for threat and the access and privilege components for vulnerability so established, a security risk level for the information system asset can be computed.

An aspect of establishing the numerical value for the threat of attack involves establishing the potential for an attack on the information system asset by a threat agent based, for example, on a combination of motivation and ability of the threat agent for the attack. Possible threat agents can be identified by either or both of a business manager or an information security officer for the entity and include, for example, casual users, kiddy scriptors, hackers, disgruntled employees, legitimate consumers, competitors, political activists, agents of organized crime, law enforcement agents, or government agents. An aspect of establishing the numerical value for the access component of the vulnerability to attack involves, for example, identifying one or more modes of access required for an attack on the information system asset by the threat agent and/or one or more methods of attack available to the threat agent. **Possible modes of access can be identified by either or both of an information security officer or a technician for the entity and include, for example, wide area network access, global network access, wireless access, proprietary network access, packet switched network access, terminal access, or physical access. An aspect of establishing the numerical value for the privilege component of the vulnerability to attack involves, for example, identifying one or more unauthorized privileges that can be acquired by a threat agent from attack on the information system asset. Possible unauthorized privileges can likewise be identified by either or both of an information security officer or a technician for the entity and include, for example, super user privileges, security administrator privileges, super user read privileges, security auditor privileges, normal user privileges, or guest privileges.**

The security risk level for the information system asset is calculated as the product of the numerical value of the threat of attack times the numerical value for the access component of the vulnerability to attack times the numerical value for the privilege component of the vulnerability to attack on the information system asset. The security risk level so calculated can be used, for example, for comparison to a security risk level calculated for another information system asset. Further, a numerical value for a security risk level threshold limit for the information system asset can be established and a security policy implemented which mandates that if the security risk level calculated for the information system asset exceeds the prescribed security risk level threshold limit, remediation shall be initiated." (emphasis added) Voss Column 4 lines 10-66.

"An aspect of the present invention defines vulnerability in terms, for example, of privileges and access. When someone exploits a vulnerability, it results in their having privileges in addition to those which they would normally have. **A normal user may be able to access certain data from a computer, but if that person were to exploit a vulnerability, he or she might have additional control, for example, to see and/or delete other persons' data that he or she would not otherwise have. Thus, vulnerability has a component of which privilege is a major part.** The other component of vulnerability is defined according to this aspect in terms of the access that is necessary for a person to have in order to exploit the vulnerability, such as whether the vulnerability presents itself to the external environment, for example, via a network or a keyboard or mouse input, or requires access for the attacking entity to the physical box itself by its floppy disc drive." (emphasis added) Voss Column 7 line 66 to Column 8 line 14.

New claim 38 recites program instructions to determine whether employees of two or more customer corporations are authorized to concurrently share use of the application and program instructions to determine whether a vulnerability in the application can be exploited by a user which has not been authenticated to the application. Program instructions assign numerical weights to the respective determinations, each of the numerical weights corresponding to a significance of the respective determination in quantifying the security risk. Program instructions combine the numerical weights to quantify the security risk. Program instructions compare the quantification of the security risk based on the combined numerical weights to a monetary value of a benefit of the application, and based on the comparison, recommend whether to certify the application for use.

None of these features of claim 38 is taught or suggested by Voss. Voss assesses a security risk based on (a) threat of attack based on possible "threat agents", (b) possible mode of access to a computer system, and (c) privilege components of one or more vulnerabilities to a computer system. The possible "threat agents" are casual users, kiddy scriptors, hackers, disgruntled employees, legitimate consumers, competitors, political activists, agents of organized crime, law enforcement agents, or government agents. The possible modes of access include wide area network access, global network access, wireless access, proprietary network access, packet switched network access, terminal access, and physical access. But, these teachings of Voss do not disclose or suggest any of the features of new claim 38.

As noted above, new claim 38 recites program instructions to compare the quantification of the security risk based on the combined numerical weights to a monetary value of a **benefit of the application**, and based on the comparison, recommend whether to certify the application for use. This feature is not taught or suggested by US 6,374,358 to Townsend or US 7,007,026 to Wilkinson (cited in the previous Office Action) either. Townsend determines "a monetary value of the **loss** to the organization if loss of the current application asset results in the business concern Ci. The loss estimate includes such factors as cost to respond, recover or rebuild the lost or damaged application asset or to recover from the side effects caused by compromise of the application asset, such as loss of market shore, loss of revenue from crippled manufacturing operations and loss of intellectual property revenue." Townsend Column 4 lines 40-52. However, this is a "damage" value in Townsend which is different than a monetary value of a benefit of the application as recited in claim 38 of the present patent application. Even the "loss of revenue from crippled manufacturing operations" of Townsend is a loss not a benefit, and is not directed to the application itself, as recited in new claim 38, but to the "crippled manufacturing operations". Wilkinson, which pertains to role-based access, does not fill this gap of Townsend. Therefore, the rejection of new claim 38 should be withdrawn.

Claims 39-43 depend on claim 38 and therefore, distinguish over Voss, Townsend and Wilkinson for the same reasons that claim 38 distinguishes thereover.

Claims 44-49 distinguish over Voss, Townsend and Wilkinson for the same reasons that claims 38-43 respectively, distinguish thereover,

In view of the foregoing, Applicants request allowance of the present patent application as amended above.

Respectfully submitted,

Dated: Feb. 8, 2011
Phone: 607-429-4368
Fax: 607-429-4119

/Arthur J. Samodovitz/
Arthur J. Samodovitz
Reg. No. 31,297